© November 2015 | IJIRT | Volume 2 Issue 6 | ISSN: 2349-6002

Cross Layer Design of Intrusion Detection in Wireless Mesh Network

Dhruvil K Patel
Silver oak college of engineering and technology
Ahmedabad, India

***Abstract*—Wireless Mesh Network (WMN) is a technology that is gaining importance among traditional wireless networks. WMN is considered as a suitable solution for providing Internet access in an inexpensive, and rapid manner. One of the main challenges in the design of these networks is their vulnerability to security attacks. Our approach is to classify existing contemporary wireless intrusion detection system (IDS) techniques based on target wireless network, detection technique. An Intrusion Detection System (IDS) detects malicious nodes in a network.**

***Index Terms*—wireless mesh network, intrusion detection system, cross layer design**

I. INTRODUCTION

The wireless communication is a service with the rapid improvement in wireless local area networks and cellular network. There are currently two variations of mobile wireless networks which are known as the infrastructured network and self-organized networks. Infrastructured is a network which has fixed and wired gateways and the bridges for these networks are known as base stations. Applications of this type of networks include WLANs. The second type is known as self-organized networks. They consist of mobile radio nodes which do not need existing network infrastructure or central system management [3]. Next generation services will provide lower equipment cost, overall flexibility on sending and receiving levels, high data rates and capacity of arriving to all subscribers. At that point, to solve all of these problems, a new concept called Wireless Mesh Network (WMN) has been proposed and it is a new technology area that will take a hand in next generation wireless mobile networks [3].

Wireless networks consists the next generation that provides better services, a key technology, and wireless mesh networks (WMNs). In wireless mesh network, nodes are comprised of mesh routers and mesh clients. Node operates as a host and a router that forward packets on behalf of other nodes that may not be within direct wireless transmission. Wireless mesh network is self-organized and self-configured. Nodes in the network establish and maintains mesh connectivity. This feature brings advantages to WMNs such as easy network maintenance, robustness, low up-front cost, and reliable service coverage [4].

II. WIRELESS MESH NETWORK

Wireless Mesh Network (WMN) is also known as wireless grid network, it is regarded as a new type of high-capacity, high-speed, broadband wireless network structure, which is counted as the next generation wireless internet.

Wireless mesh network are not built on a fixed infrastructure and hosts rely on each other to keep the connection so that WMNs provide low-cost broadband internet access. LAN coverage and network connection are fixed for network operators and users. WMNs is easy, fast and deployment of the technology. WMN consists of mesh routers and mesh clients. Mesh routers are fixed and they are connected with wireless infrastructure and work with the other networks to provide internet access service for mesh clients. Over the mesh routers and clients Mesh clients can connect to network. Due to large number of nodes, there occurs some issues like security, scalability and manageability is required. [3]

Infrastructure / Backbone WMNs:

Infrastructure WMN architecture is shown in Figure. In this WMNs it consists interconnecting clients. Routers, internet and other clients can be connected by cables (as shown with straight lines) or wireless links (as shown with dashed lines). WMN backbone uses IEEE 802.11 technology within various wireless technologies. Infrastructure/Backbone WMNs are the most commonly used type. For example, community and neighborhood networks can be built using infrastructure meshing. The mesh routers are placed on the roof of houses in a neighborhood, which serve as access points for users inside the homes and along the roads. Typically, two types of radios are used in the routers [3].

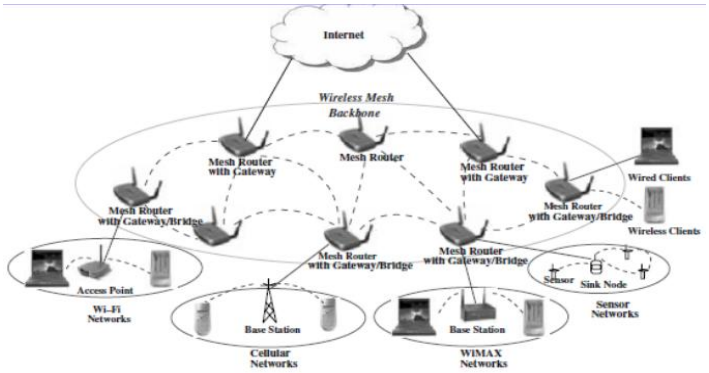


Fig. 1: Infrastructure/backbone WMN [3].

Client WMNs:

There is not necessary of router on the networks which are established between clients as P2P. Highest level of data transmission occurs in the client wireless mesh network. To reach a destination through multinodes a packet is sent and the traffic crosses over single nodes in the network. All Nodes require to have routing and self-organization functionalities in this WMNs [4].

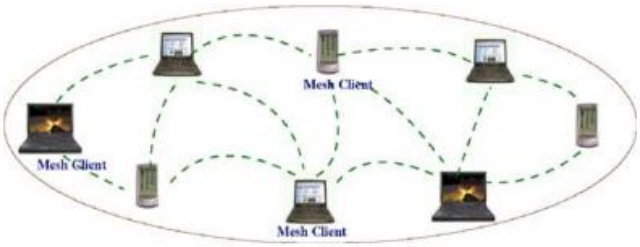


Fig 2 Client WMN [4]

Hybrid WMNs:

Mesh network can be covered by an additional network structure and that controls long-distance packet traffic. As shown in Figure hybrid WMN has infrastructure and client WMNs and the infrastructure part provides the connection between mesh and the internet, Wi-Fi and WiMAX networks; the clients' part organizes routing processes [3].

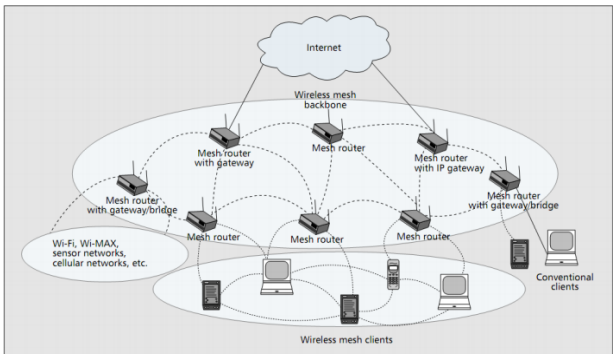


Fig 2 Hybrid WMN [3]

Characteristics of wireless mesh network

- Multi-hop wireless network.
- Support for ad hoc networking, and capability of
- Self-forming, self-healing, and self-organization.
- Mobility dependence on the type of mesh nodes.
- Multiple types of network access.

III. INTRUSION DETECTION SYSTEM

Any action that try to compromise the integrity, confidentiality or availability of a resource or that goes against the security goals of a resource that is called intrusion. Try to attack confidential data or misusing the email system for spam is one type of try to attack on system. Intrusion attempts are incorrect routing information, prevent services from working properly or shutdown them completely are called external attempts. The internal intrusions could occurs a lot more damaging. There is not always possible Intrusions prevention, there is a need to supportive intrusion detection techniques. Intrusion detection systems (IDSs) are not to prevent or deter attacks. The purpose of intrusion detection system is to alert the users about possible attacks and ideally in time to stop the attack or control the damage. An IDS reaches perfection if it regularaly detects attacks and hardly makes any false or phantom detection. One basic assumption while designing any IDS should be that the attacker is intelligent and that the attacker has no shortage of resources [10].

Types of intrusion detection systems

There are two types of intrusion detection systems.

1. Network Based Intrusion Detection system (NIDS) which resides on network.
2. Host Based Intrusion Detection system (HIDS) which resides on host i.e. computer system.

Network Based intrusion detection system (NIDS)

In the Network based intrusion detection system it resides on network. On hardware system it exists as software process. Into promiscuous mode, it change the network interface card (NIC). i.e. The card can be pass through all traffic on the network to the NIDS software. In the software rules are used to analyze the traffic. The incoming packets are analyzed against these rules to determine the signature of the attacker, whether in this traffic signature is of any attacker or

not. If there is an attacker then events are generated. The data source to NIDS is raw packets and It utilizes a network adapter which is running in promiscuous mode to monitor and analyze the network[15].

Host Based Intrusion detection system (HIDS)

Host based IDS resides on host computer and it exists as a software process on a system. HIDS examines the log entries in system for information and it identifies the new entries and compares them with rules. It works on rule based, if the entry match with rule then it will generate alarm that this is not legal user [15].

Intrusion Detection System for WMN

IDS designed for multi-hop wireless networks are mostly based on the characteristics of MANET such as follows:

Temporary network which has no support of routers and gateways; instead the nodes also perform the routing functionality.

Application specific which is used mostly for emergency situations such as natural disasters or battle fields.

Served by mobile nodes which possess power and bandwidth constraint.

The traffic pattern is from users to users. The existing cooperative and hierarchical IDS are MANET based.

The intrusions detection and monitoring mechanisms are implemented in MANET nodes and These IDS ensures the cooperation amongst the MANET nodes to collectively monitor the intrusions and in case of intrusion found, then inform each other, or the cluster head which is responsible for intrusion detection of all its child nodes. Furthermore there is no question of involvement of the routers and gateways in MANET IDS.

As compared to MANET, the WMN has significant different network characteristics, that is why, proposing or investigating any IDS, there is a need to keep under consideration the characteristics of WMN [11]

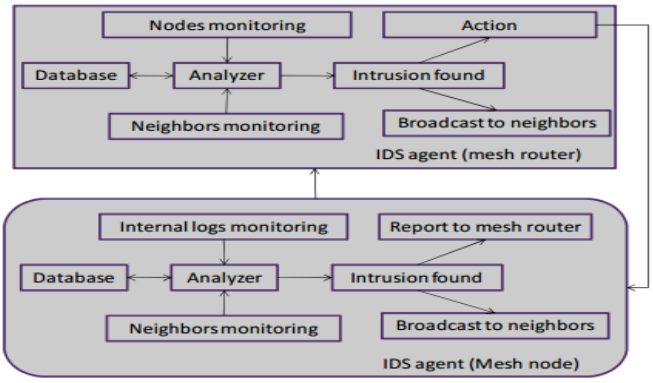


Fig 4 IDS for WMN [15]

IV. CROSS LAYER DESIGN

Cross-layer design emphasizes on the network performance optimization by enabling different layers of the Communication stack to share state information or to coordinate their actions in order to jointly optimize network performance. So that the concept of cross layer design must be compared with the traditional layered architecture and people can be motivated towards the use of the violation of the layered design [14].

Definition of a cross -layer design is given as any modification of the layered reference architecture. The intent of cross layer design, simply stated, is to exploit information from multiple layers to jointly optimize performance of those layers. The breaking of hierarchical layers or the violation of reference architecture includes joining of layers, creating a new interfaces, or providing additional interdependencies between any two layers as shown in Figure

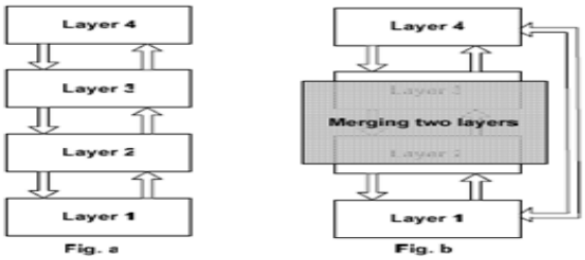


Fig 5 Reference architecture with interfaces and violation [14]

V. CROSS LAYER BASED TECHNIQUE

Cross layer based technique is used to make decision that whether there is an attacker or not by combining the result of two or more layer in TCP protocol.

Monitoring Received Signal Strength (RSS)

A measure of energy which is observed by the physical layer at the antenna of the receiver is called as Received signal strength (RSS). The radio equipment used by the receiver have to be same for identify exact value of RSS. Moreover there should be same level of reflection, refraction, and interface. Even if the sender is fixed, RSS value seems to vary a little and it is proved that it is almost not possible to guess. This restricts the attacker from using the radio equipment to spoof the RSS clearly by the receiver.

Any sudden or unusual changes can be marked as doubtful activity which indicates the possible session of hijacking attack. Reason why one call RSS profile dynamic is because during every session it is built again and keep on updating. Any sudden changes in the RSS dynamic profile can be marked as doubtful activity with a higher confidence level because BSs are generally immobile. On the other hand, if the MS is mobile, then its respective RSS values will vary quickly which can be observed by the server.[9]

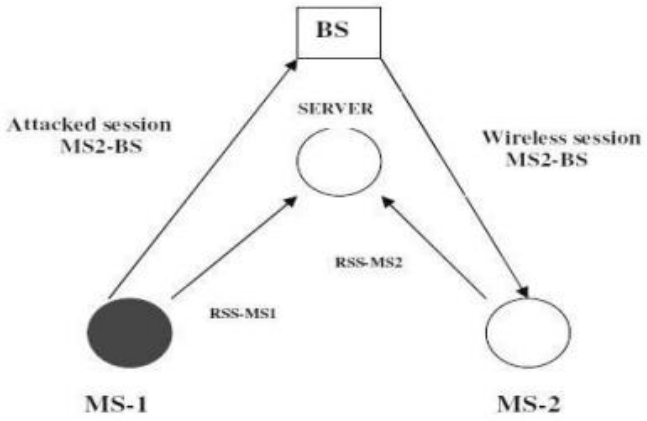
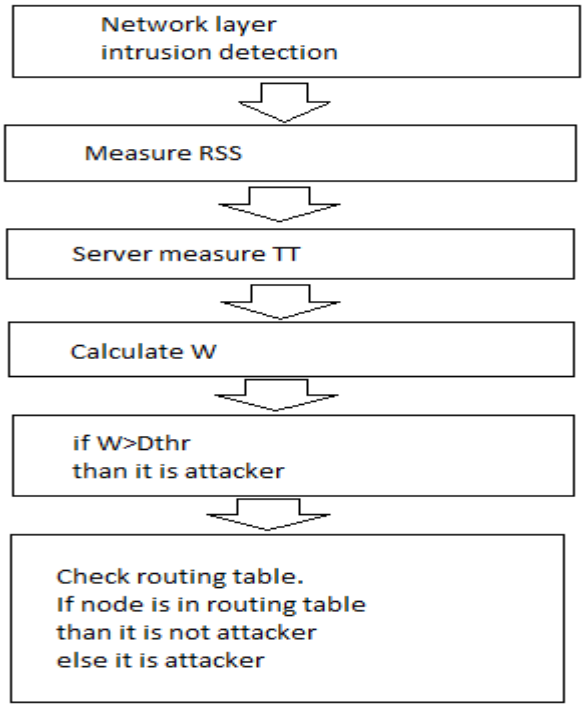


Fig 6 Received signal strength (RSS)[9]



VI. DETECTION ALGORITHM

Step 1: Server measures RSS.
Step 2: Server measures TT.
Step 3: Server calculates the weight W as:
$W = w1.\delta RSS + w2.\delta TT$
Where δRSS=variation of RSS and δTT=variation of TT, w1 and w2 are two constants, which can be fine tuned.
Step4: If W>Dthr, (where Dthr is the detection Threshold) then: MS is an attacker.
Step 5:Check routing table.
If node is in routing table it is not attacker
Else it is attacker
By suitably adjusting the values of Dthr, and w1 and w2, we can reduce the false positive rate, significantly.

VII. RESULTS

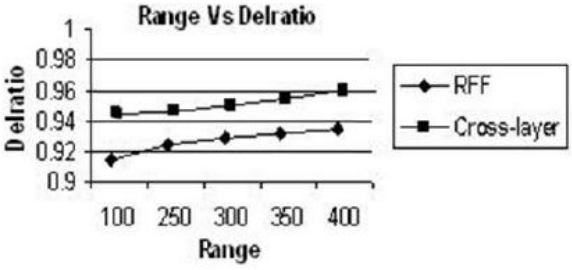


Fig 7 Result of base paper

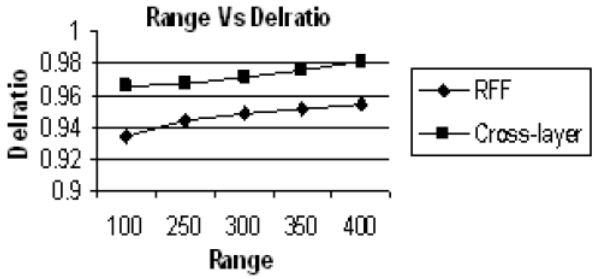


Fig 8 Result of our experiments

REFERENCES

[1]Divya Bansal, Sanjeev Sofat "Use of Cross Layer Interactions for Detecting Denial of Service Attacks in WMN" 978-1-4244-6705-1/10/$26.00 ©2010 IEEE,

[2]Felipe Barbosa Abreu, Anderson Morais, Ana Cavalli, Bachar Wehbi, Edgardo Montes de Oca Montimage,An Effective Attack Detection Approach in Wireless Mesh Networks , 978-0-7695-4952-1/13 $26.00 © 2013 IEEE , pp.1450-1455.

[3] Safak DURUKAN ODABASI, A. Halim ZAIM2, "A SURVEY on WIRELESS MESH NETWORKS, ROUTING METRICS and PROTOCOLS" INTERNATIONAL JOURNAL OF ELECTRONICS, MECHANICAL and MECHATRONICS ENGINEERINGVol.2 Num.1 pp.(92-104)

[4] Ian F. Akyildiz, Xudong Wang, Weilin Wang "Wireless mesh networks: a survey" I.F. Akyildiz et al. / Computer Networks 47 (2005) pp 445–487

[5I ANF. AKYILDIZ, XUDONGWANG, "A Survey on Wireless Mesh Networks," IEEE Radio Communications • September 2005, pp. 523-530

[6] Aggeliki Sgora, Dimitrios D. Vergados, and P. Chatzimisios "A Survey on Security and Privacy Issues in Wireless Mesh Networks"

[7] Ratika Sachdeva, Aashima Singla,"Survey on Privacy Issues and Security Attacks in Wireless "Sachdeva et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(4),April - 2013, pp. 463-467

[8] Parth H. Pathak, Rudra Dutta." A Survey of Network Design Problems and Joint Design Approaches in Wireless Mesh Networks" pp. 1-41

[9] Robert Mitchell, Ing-Ray Chen." A Survey of Intrusion Detection in Wireless Network Applications" January 19, 2014.pp 1-30

[10] Novarun Deb, Manali Chakraborty, Nabendu Chaki." A State-of-the-ar t Sur vey on IDS for Mobile Ad-Hoc Networks and Wireless Mesh Networks"

[11] Shafiullah Khan, Kok-Keong Loo, Zia Ud Din," Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks" The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.pp 435-440.

[12] Tiranuch Anantvalee, Jie Wu." A Survey on Intrusion Detection in Mobile Ad Hoc Networks"pp 170-196.

[13] Novarun Deb, Manali Chakraborty, Nabendu Chaki." THE EVOLUTION OF IDS SOLUTIONS IN WIRELESS AD-HOC NETWORKS TO WIRELESS MESH NETWORKS" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.pp 39-58.

[14] Mr.M.D.Nikose. "A REVIEW OF CROSS LAYER DESIGN" International Journal of Emerging Trends in Engineering & Technology (IJETET) Vol. 02, No. 01, 2013.pp 7-18

[15] Dr. Vinod Kumar, Mr Avtar Singh, Mrs. Ritika Narang." PERFORMANCE ANALYSIS OF EFFECT RATE OF CROSS LAYER BASED INTRUSION DETECTION FOR WIRELESS LAN" International Journal of Computers & Technology. Volume 5, No. 2, May -June, 2013.pp 80-84.

[16] Meijuan Gao, Jingwen Tian." Wireless Sensor Network for Community Intrusion Detection System Based on Improved Genetic Algorithm Neural Network"pp 199-202.

[17] Xia Wang, Johnny S. Wong, Fred Stanley and Samik Basu." Cross-layer Based Anomaly Detection in Wireless Mesh Networks" 2009 Ninth Annual International Symposium on Applications and the Internet. pp 9-15.

[18] Yatao Yang, Ping Zeng, Xinghua Yang, Yina Huang." Efficient Intrusion Detection System Model in Wireless Mesh Network"2010.pp 393-396.

[19] Juliette Dromard, Rida Khatoun, Lyes Khoukhi." A Watchdog Extension Scheme Considering Packet Loss for a Reputation System in Wireless Mesh Network"